报业网络和互联网统一出口双活及安全建设浅析

金建明
（温州日报报业集团，浙江 温州 325000）

摘要：【目的】为了提高报业集团网络和互联网出口链路高效、双活、安全。【方法】温州日报报业集团创新使用拎篮子方式实现各出口业务在负载均衡设备上的灵活组合；并在交换网络上采用 DRNI 跨设备链路聚合技术，不但实现链路双活、聚合，同时具有高负载均衡和安全性。【结果】能快速排查各类网络安全威胁并及时处置，轻松应对局部业务受攻时对集团整个网络出口的影响。【结论】项目建成后在温州日报报业集团网络及出口安全运维中取得良好的效果，同时对报业同行建设高效、安全、双活的网络及互联网出口具有一定的参考和借鉴意义。

关键词：带宽；冗余；双活；负载均衡；拎篮子　　中图分类号：TP393.08　　文献标识码：A
文章编号：1671-0134（2023）06-045-05　　DOI：10.19483/j.cnki.11-4653/n.2023.06.031
本文著录格式：金建明 . 报业网络和互联网统一出口双活及安全建设浅析 [J]. 中国传媒科技，2023（06）：145-148.

1. 温州日报报业集团改造网络和出口安全的必要性

2007 年，温州日报报业集团（以下简称“集团”）引进了不同运营商的 3 条互联网光纤（电信 1G、网通 1G、移动 500M），并配备了负载均衡设备作为集团互联网统一出口，集团内部上网和外部对集团所有网站、视频、新媒体等访问都是通过这 3 条光纤。因为只有一个统一的出口，任何一个网络异常都有可能影响到集团全局的网络访问，这对集团出口的设备安全、高效、稳定提出很高的要求。当时，采用统一出口的报业集团几乎没有，大都是把内部办公对外和外对内 DMZ 区访问分别部署成两个完全独立的互联网出口，互不干扰。

1.1 原有集团网络和出口安全设备性能

2 台 F5 负载均衡设备和 2 台 Juniper 防火墙，这些设备只做双机热备，没有双活，网康上网行为设备串在它们中间（存在单点故障）；防火墙下联 2 台热备 Extreme 8810 核心交换机；防火墙另一下联为千兆 WAF 防火墙，再由 WAF 连接到 DMZ 汇聚交换机。由于当前网络威胁和攻击日益增多，温报集团 10 多年前购买的网络和安全设备已不能满足高强度的防护要求，须对集团网络和出口安全进行改造。

1.2 原架构痛点：做不到双活、带宽不够

原出口网络和出口安全设备采用主备架构，这种方式所有的业务和流量只能由一台主用设备硬扛，备用设备无法在线分担，集团某一网站一旦受大流量攻击，会连累到整个内到外的上网速度及集团其他没被攻击网站的访问网速，甚至中断，极大影响正常的出版和其他网站的对外业务；原网络和安全设备的接口速率均为 1G，当访问总流量高峰超过 1G 时有可能造成网络拥塞。此外，个别设备还存在单点故障的风险。

2. 新网络和互联网出口建设思路

新网络和出口必须解决上述痛点，既要做到安全同时又要双活，还要做到负载均摊。

双活要求每个设备至少都要双份，如果在互联网出口前端像葫芦串一样加一大串的双份安全设备，不但购买成本非常高，且对双活造成很大的困扰，这就要求选择设备时尽可能要减少设备数量，在一个设备上集成尽可能多的应用。因此，笔者所在团队的建设思路是：在达到功能要求的前提下，尽可能用较少的设备做到在线双活；其次是统计分析功能要足够强大和细致，有利于日后网络优化和排错。

核心网络和安全设备接口从原来的 1G 全部提升到万兆，同时把所有垂直干线提升到万兆，水平布线全部达到 1G。对所有网络设备要能做到跨设备链路聚合，提高链路的稳定性，又能做到链路的负载均摊，同时具有灵活的端口镜像功能。

对防火墙的要求除具有防火墙基本功能外，还要具有较强的入侵防御系统、威胁检测模块，能够快速发现网络威胁来源并加以拦截。

负载均衡设备是部署在最前端，除链路和服务器负载均衡功能外，抗 DDOS 功能和访问加速功能也要有。

WAF 设备能对网站访问进行全方位的智能防护，能自动识别和阻断各种扫描行为。同时还要有智能学习、

智能锁定攻击者、防止篡改监控等功能。所有网络与安全设备要能纳入 IT 运维管理系统，方便日后运维。

3. 新设备功能特点

此次集团引进的新设备是网神 NSG7000-TX10M-Q 新一代防火墙和 A10 TH3030S 负载均衡各 2 台、安恒 WAF-3000AG1 台、H3C 网络设备进行全网更换。新设备上线保持集团网络总体大的架构基本不变，稍做如下微调：由于新的设备全是万兆接口，网康千兆设备不再适用串接，移到核心交换机做旁路挂接；同时，也避免了单点故障。改造后的集团网络拓扑图（如图 1）。

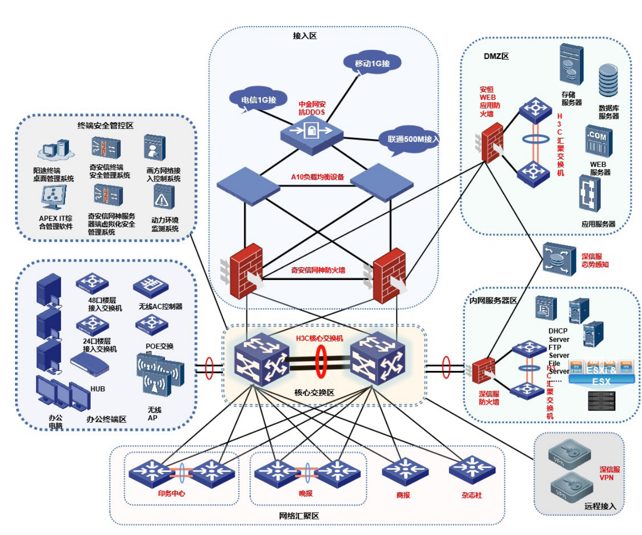


图 1　改造后的集团网络拓扑图

3.1　支持 DRNI 技术的 H3C 交换机

DRNI（Distributed Resilient Network Interconnect，分布式弹性网络互连）作为一种跨设备链路聚合的技术，从而把链路和设备的可靠性从单板级提高到设备级。[1] 本次温州日报报业集团采用 H3C 的 S10510X 核心、LS-7503E 等汇聚、S5130 等楼层交换机均支持 DRNI 技术进行链路聚合，大大简化了组网和配置，既提高了带宽，又提高了链路的稳定性，同时还能做到链路的负载均摊。核心采用先进的 CLOS 多级多平面交换架构，可以提高带宽的持续升级能力，能够适应不同网络规模的端口密度和性能要求。

新核心交换机交换容量 ≥ 700Tbps，包转发率 ≥ 96000Mpps，光纤接口全万兆（最高支持 100GE），比原来的 Extreme 核心各项性能提升了 10 倍；支持双向 ACL、支持端口 ACL，支持 VLAN ACL，符合集团原用 ACL 技术对各子报的访问权限进行隔离和控制的技术要求。

3.2　多功能一体防火墙

防火墙作为一种边界安全设备，所起的作用是对内、外部网络实施隔离，一方面尽可能屏蔽内部网络结构，另一方面尽可能屏蔽外部威胁，以拦截外对内的非法访问。在安全漏洞频出、网络攻击肆行的今天，引进一套高带宽、高性能、集多种功能模块于一体的新一代防火墙尤为重要。

网神 NSG7000-TX10M-Q 新一代防火墙具有 42Gbps 吞吐量，除了常规 NAT、协议识别等功能，还具有入侵防御检测 IPS 模块、病毒检测防毒网关、态势感知、僵尸主机检测、威胁云检测等应用模块，大幅提升了边界安全防护能力。

新网神防火墙的监控指标比较多：会话数、流量数、各种威胁数量、各协议应用占比等，日志分析功能比较强大，结果呈现清晰明了。针对某一时段的网络异常事件，通过各异常指标的追查，最终都能找出相对应的主机和 IP，进而进行规避。

3.3　集抗 DDOS、应用加速为一体的 A10－TH3030S 负载均衡

TH3030S 四～七层的吞吐量都 ≥ 30Gbps、最大并发连接 ≥ 2000 万、万兆接口 ≥ 6 个，并具有抗 DDOS 和应用加速功能。该负载均衡能支持流量图形化展示，该功能对网络排错非常管用。

3.4　高性能网站应用级入侵防御 WAF 系统

新上线的安恒 WAF-3000AG 应用层吞吐 ≥ 8Gbps、并发连接数 ≥ 40 万、每秒新建连接数 ≥ 4 万、业务时延小于 50ms、防护站点无限制。

新 WAF 具有 CC 防护功能；能够识别跨站脚本（XSS）、注入式攻击等恶意请求应用攻击行为；支持对 HTTP 请求分割攻击和 HTTP 响应报文截断攻击的防护；能基于访问行为特征进行分析，具有识别盗链、爬虫攻击的能力；能识别网站中的网页木马程序，通过策略可防止木马网页被用户访问。

4. 项目的创新点：首创拎篮子式双活架构

本项目对集团出口安全设备进行创新设计，双活架构，避开原系统的痛点。首创把出口业务按种类分块（即篮子）技术成功应用于出口的网络攻击应急，避免了受攻击网站对其他正常业务的影响。按业务的性质把内外网访问通道分成 4 个篮子：篮子 A 装的内对外的上网业务，篮子 B 装的是各报网刊的对外网站业务，篮子 C 装的是温州网二套（各服务对象的网站业务），篮子 D 装的是平时比较容易受攻击的温州网主站。这 4 个可以按任意组合运行在 2 台 A10 负载均衡设备上，平时一般是每台 A10 上各跑 2 个篮子（如图 2）。假设当 D 篮子网站受到攻击时，可以将 D 篮子独自在一台 A10 上运行，另 3 个没受到攻击的篮子全部跑在另一台 A10 上，不会受攻击的影响，最大限度保证其业务正常（如图 3）。甚至还可以把 2 台防火墙进行分离，把统一出口分割成互不相干的 2 条出

口链路，让受攻的篮子 D 完全从独立链路出去，彻底解决互相干扰问题（如图 4）。2021 年集团一网站受到 DDOS 大流量攻击，团队也是通过此方法进行处置，基本上没有对其他正常业务造成影响。

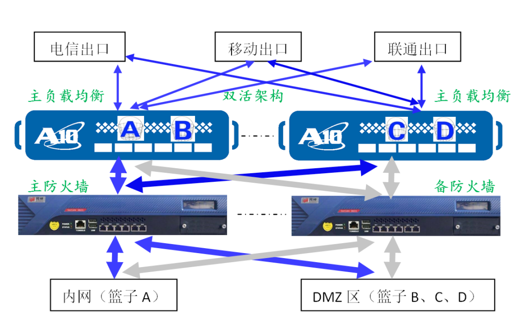


图 2　正常情况下集团出口流量示意图

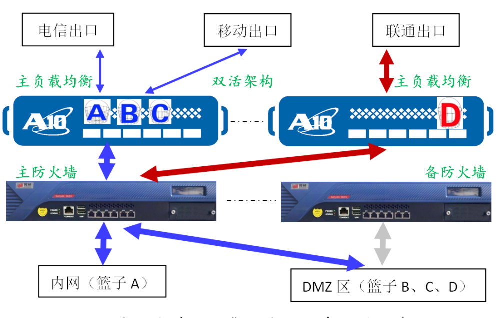


图 3　受攻击情况下集团出口应急流量示意图

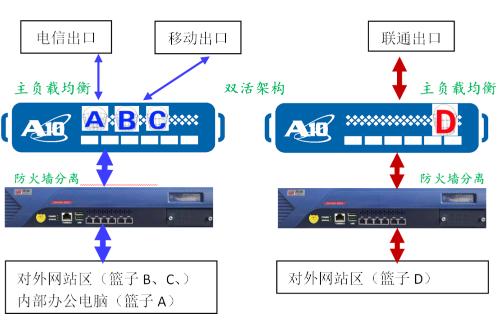


图 4　统一出口彻底分离业务示意图

5. 应用实例

5.1　快速查明“未知”流量攻击

在新设备上线之前的一段时间，集团网络出口网络偶尔会出现不定时的一两分钟中断。由于 10 多年前购买的原负载均衡设备和防火墙监测、分析功能不是很强；再加上出问题的时间不固定，很难抓包分析，所以一直查不出原因，甚是困惑。新设备上线后利用 A10 的网络指标图形化展示功能很快解开了这个困惑，当出现大流量攻击时，团队查阅了当时的网络波形图，发现电信出口 1G 带宽被大流量打满（如图 5），A10 上接联通、移动网口及下联防火墙 e9 网口并没有出现大流量，于是很快就能断定断网流量来自电信线路的外部攻击。但是针对集团内部的哪一台服务器进行攻击呢？团队又在 A10 的虚拟服务器（每个虚拟服务器对应着一台实体服务器）中找该同一时段内与图 5 相反的流量图形（如图 6），图 6 的 99.27 服务器流量和并发先是突然暴增，紧接着就是下降到零，很符合被攻击然后断网这一特征。于是很快查明是基于 UDP 123 端口的网络时间协议（NTP）NTP–flood 攻击，通过相应的防护手段，问题得以解决。[2]

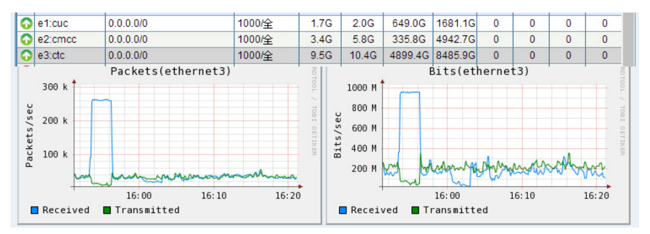


图 5　NTP–flood 攻击时电信出口网络流量图

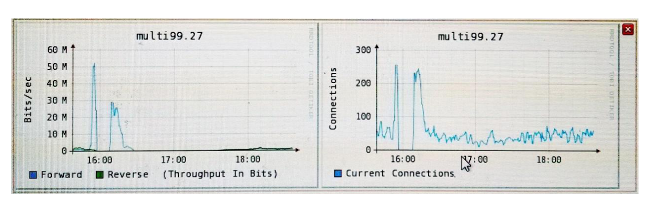


图 6　NTP–flood 攻击时被攻服务器网络流量图

5.2　快速识别内网高风险主机

集团内网有 1500 多台电脑，个别电脑防护不到位，被植木马或被操控都是有可能的，以前团队想要得知哪些是内网高风险电脑，只能通过网康上网行为设备中的流量 TOP10 等判定主机是否异常，但这种判定误判率太高。现在的网神防火墙中具有态势感知、僵尸主机检测、威胁云检测等功能，能从流量、并发数、协议、端口等多维度直接判定哪些可能是高风险的失陷主机，并直接列出来（如图 7）。


失陷主机视图 | IOC列表视图

待响应失陷主机数：54　阻断失陷主机数：0　仅记录日志失陷主机数：0　忽略失陷主机数：135

响应　撤销　忽略　删除　刷新　全部展开　全部折叠　最近7天

失陷主机/IOC	描述	命中数	动作	最近发现时间	首次发现时间	来源	用户名
172.29.21.20		0	待响应	2018-05-19 21:03:48	2018-05-19 21:02:28		
bigdata.adfuture.cn	普通远控木马活动事件					本地	
172.30.1.50		0	待响应	2018-05-19 01:18:34	2018-04-17 16:28:10		
serve.popads.net	Minerd挖矿木马活动事件					本地	
172.27.4.75		0	忽略	2018-05-18 20:36:42	2018-05-18 20:35:56		
coinhive.com	MinerdPool矿池异常访问事件					本地	
172.27.2.152		0	忽略	2018-05-18 19:35:55	2018-02-26 22:44:34		
bigdata.adsunflower.c...	普通远控木马活动事件					本地	
bigdata.advmob.cn	普通远控木马活动事件					本地	
bigdata.adfuture.cn	普通远控木马活动事件					本地	

图 7　集团内网失陷主机列表

团队按图 7 的 IP 对这些电脑进行清查，大部电脑是真的存在一些问题的，但发现 172.27.4.75 并非真的失陷，因为该机是一台域控 +DHCP 服务器，访问的并发数、流量等超过一定的额度，从而也被归入失陷的名单，把该机添加到白名单中即可。

5.3　利用防火墙查明一起因 DDOS 防护引起的流媒体调用失败案例

2022 年 1~3 月间，出现过 3 次 DMZ 区一 App 服

务器调用内网视频服务器的视频流出现时断时续或中断的现象，由于该 App 服务器需经过 DMZ 汇聚交换机→ WAF 防火墙→出口防火墙→核心交换机→内网防火墙→才能访问到内网服务器，由于其是 80 端口调用，在每次出现故障时，把 WAF 直通或重启都能奏效（实际上相当于是把链路重置了一遍），大家都以为是 WAF 拦截的原因，但奇怪的是在 WAF 上找不到任何相关的日志。后在出口网神防火墙分析中心查到其调用失败期间有大量 HTTP 流媒体威胁告警（如图 8），随后在下次出现同样故障时及时在防火墙上抓包，发现有大量的请求包到防火墙，但到达内网视频服务器的却很少，初步判定是包被防火墙拦截并丢弃了。在防火墙的数据中心发现 App 服务器请求命中的是 rb-front-web-2 策略，继而查明该 App 服务器到内网视频服务器的访问请求中使用了 HTTP 协议、GET 请求，URL 中带有（flv、mp4）这 2 种视频类型的流量，当流量数据过大时触发 rb-front-web-2 策略中的抗 DDOS 功能，导致该 App 服务器发出的请求数据包被丢弃，从而出现业务间歇性中断。后调高 rb-front-web-2 策略中的 DDOS 阈值，问题暂时得以解决。

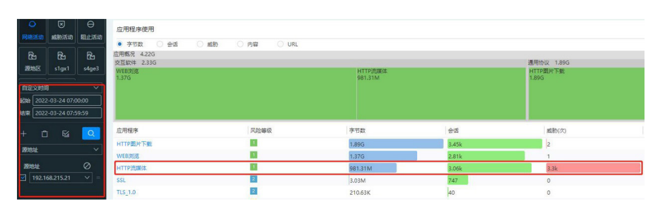


图 8 通过防火墙的分析中心发现大量 http 流媒体威胁告警

5.4 解决了 VLAN 翻转时可能出现的断网，网络交换更高效、稳定

集团原 EXtreme 交换机采用 ESRP 协议（类似 VRRP）体系，核心采用主备模式。由于各报网刊按业务功能会分成多个 VLAN，其中有一个是主 VLAN，各从 VLAN 都会随着主 VLAN 在主备核心交换机上漂移而漂移。假如 A 楼层到主交换机的链路出现故障时，会将本报主 VLAN 的 master 迁移到备核心交换机上，同时把本报的所有从 VLAN 也漂移到备核心交换机上，此时如果 B 楼层到备核心交换机上有链路不通，且 B 楼层的交换机上也有该报的 VLAN，就会造成 B 楼层的交换机无法连上备核心交换机而断网。团队这次采用了 DRNI 跨设备链路聚合组后，对楼层上行到核心的双链路进行捆绑后接入到 S10510X 核心交换机，很好地解决了此类断网的问题，同时又提高了带宽。任何一楼层交换机断开上行双线中的任何一条都不影响本楼层和其他楼层的网络正常使用。

5.5 轻松搞定端口镜像，解决其他安全设备数据来源问题

原核心交换机只能支持多对一端口镜像，没办法实现多个镜像口，对上网行为和态势感知等旁路接入很不方便。本次引进的 H3C 交换机支持多对一、一对多、多对多端口流量镜像，为集团的态势感知设备、上网行为管理设备、数据抓包等接入提供丰富的端口镜像支持。

结语

本次建设原本想把防火墙也做成双活，更有利于负载的分担，但防火墙的下连线路过多，监测的链路死活和链路切换过程过于复杂，怕整个出口网络混乱，导致莫名的故障，只好放弃防火墙双活。

温州日报报业集团是较早就把内对外访问和外对内访问合二为一报业集团，这种构架的网络出口，一旦集团的某一网站被攻或流量异常，会影响到整个集团内所有用户的对外访问，甚至中断。之前也曾网站受到DDOS等攻击造成集团整个出口断断续续的情况。此次集团网络和出口相关安全设备采用双活架构并实现负载均衡，解决了多年来一直困扰集团的网络交换和出口安全的痛点。同时，新购的设备在性能上、功能上、安全性上都有很大的提升，防火墙和 WAF 每年拦截威胁各超 4 亿次，能很好地适用当前网络威胁多、新闻网站易受攻的复杂网络环境。自启用以来很好地保障了集团网站和网络的安全，很好地保驾了中国共产党成立 100 周年、党的二十大等期间温州日报报业集团网络的安全。

参考文献

[1] 跨设备链路聚合——一篇文章带你了解跨设备链路聚合 DRNI 技术 [EB/OL]. 中国专业 IT 社区 CSDN，https：//blog.csdn.net/weixin_39664998/article/details/111364209，2020-11-19 /2023-03-25.

[2] NTP 放大攻击 [EB/OL]. 博客园（开发者的网上家园），https：//www.cnblogs.com/autopwn/p/14694221.html，2021-04-23/2023-03-13.

作者简介：金建明（1974-），男，浙江苍南，高级工程师，研究方向为计算机、网络、音视频等系统集成的项目管理、规划设计及建设。

（责任编辑：张晓婧）